IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TENNESSEE

IN THE MATTER OF THE SEARCH OF ELECTRONIC DEVICES CURRENTLY LOCATED AT CONTAINER "EV", OSI DETACHMENT 106, ARNOLD AIR FORCE BASE, TENNESSEE, 37389	Case No. ~~4:23-MJ-~~ 1:23-mj-191

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH

I, Special Agent Trevor Osborn, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices—seized during search warrants of BRENT DESALVO's ("DESALVO") residences further described in Attachment A, which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I have set forth only the facts I believe are necessary to establish probable cause to believe that contraband, evidence, fruits, and instrumentalities of violation of 18 U.S.C. § 641, are presently located on DESALVO's devices.

3. I am a Special Agent with the Office of Special Investigations (OSI). My duties as a Special Agent include conducting felony level criminal and counterintelligence investigations by authorities outlined in Title 10 U.S.C § 9013; Public Laws of Congress – PPL 99-145; Title 28 U.S.C § 535 Section (c)(1). As such, under Title 18 U.S.C § 3105; Title 18 U.S.C § 3106 and 28

CFR 60.3, I am empowered by law to execute and serve any warrant or other process issued under the authority of the United States (including search warrants), for any felony cognizable under the laws of the United States if I have probable cause to believe that the person in question has committed or is committing the felony, or property relating to the investigation of a felony offense contains evidence of the crime committed.

4. I have been a Special Agent with OSI since July 14, 2020. I received training to be an OSI Special Agent at the United States Air Force Special Investigations Academy (USAFSIA), Basic Special Investigators Course (BSIC) and the Federal Law Enforcement Training Center (FLETC), Criminal Investigator Training Program (CITP), Glynco, GA. As an OSI Special Agent, my mission is to identify, neutralize and exploit criminal, terrorist, and intelligence threats to the Department of the Air Force (DAF), Department of Defense (DoD), and United States Government. In my capacity as a Special Agent with OSI, I have investigated numerous federal crimes under Title 10 of the United States Code (the Uniform Code of Military Justice [UCMJ]) and Title 18 of the United States Code, which have included fraud, sabotage, sexual assaults, sexual assault against minors, aggravated assault, child pornography, and other counterintelligence offenses. During my career, I have received formal education and training on the concepts of probable cause and reasonableness for searches and seizures that conform with the application of the 4th Amendment of the U.S. Constitution.

5. As set forth in more detail below, I believe there is probable cause that BRENT DESALVO is involved in Theft of Government Property in violation of the above listed United States Code. I further believe the electronic devices to be searched, as set forth in Attachment A, contain instrumentalities, contraband, and evidence of these crimes, as set forth in Attachment B. As described in detail below, the investigation has revealed these devices were used in furtherance

of criminal conduct, and in violation of communications security (COMSEC) and information security (INFOSEC) DoD policies, and it is believed they will contain evidence of this conduct. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

6. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

DEFINITIONS

7. The following definitions apply to this affidavit and Attachments A and B:

a. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

b. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory

storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

c. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

d. The "Domain Name System" or "DNS" is a system that translates readable Internet domain names, such as www.justice.gov, into the numerical IP addresses of the computer server that hosts the website.

e. "Encryption" is the process of converting data into a code to prevent unauthorized access to the data.

f. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

g. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

h. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

i. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static" if an ISP assigns a user's computer a particular IP address that is used each time the computer

accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

j. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device, contain a digital camera capable of recording photographs and videos, and capability for storing electronic data.

k. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include

various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

l. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

m. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

n. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

o. "Key Variable Loader" and "Key Variable Loader 4000" as used herein refers to a device used to encrypt radio channels. The KVL-4000 encryption Key Variable Loader for secure enabled Motorola products is equipped with the MC55 Personal Digital Assignment (PDA). This PDA style key loader is outfitted with features and a user interface for increased efficiency and programming flexibility. A large LCD color display paired with an easy-to- use alphanumeric keypad enables simple viewing and data entry. Built with legendary Motorola quality and security, the KVL-4000 is built to withstand everyday use in Federal and public safety environments. The KVL-4000 automatically generates random keys for any algorithm and can auto-generate a single key or a bulk set of keys. FIPS provides the highest level of security for data; User timeout automatically logs out the user after a specified period of inactivity; User and administrator authentication allow users and administrators to perform and restrict firmware upgrades, changes, and key management.

p. "Trunk System" or "Trunking System" as used herein, refers to a trunked radio system, which is a two-way radio system that uses a control channel to automatically assign frequency channels to groups of user radios. In short, trunked radio systems allow multiple groups of users to share a small set of radio frequencies without accidentally hearing or talking over each other's conversations.

q. "Code Plug" as used herein, refers to a file that contains all the programming information for a radio. It defines not only the frequencies on which a radio can transmit and receive, but also which talk groups that the radio can communicate over, as well as other operating parameters.

r. "Astro 25", "Project 25 (P25)" and "Astro P25" as used herein, refers to Motorola Solutions Project 25 (P25), a standard system developed by and for public safety professionals and adopted by federal agencies. It ensures that systems deliver the interoperability and dependability. The U.S. Federal government requires P25 compliance for most grant applications and numerous agencies around the globe have mandated P25 for all new equipment.

s. "Radio Equipment" as used herein, refers to an electrical or electronic product, which intentionally emits and/or receives radio waves for the purpose of radio communication and/or radio determination, or an electrical or electronic product which must be completed with an accessory, such as antenna, so as to intentionally emit and/or receive radio waves for the purpose of radio communication and/or radio determination; any equipment or apparatus designed or used for radio communications.

t. "Land Mobile Radio (LMR)" equipment and systems as used herein, refers to terrestrially based, wireless communications systems commonly used by federal, state, local, tribal, and territorial emergency responders, public works companies, and the military to support voice and low-speed data communications. LMR systems typically consist of handheld portable radios, mobile radios, base stations, a network, and repeaters.

- Handheld portable radios are carried by personnel and tend to have a limited transmission range.
- Mobile radios are often located in vehicles and use the vehicle's power supply and a larger antenna, providing a greater transmission range than

handheld portable radios.

- Base station radios are located in fixed positions, such as public safety answering points or dispatch centers, and tend to have the most powerful transmitters.
- A network is required to connect the different base stations to the same communications system.
- Repeaters are used to increase the effective communications range of handheld portable radios, mobile radios, and base station radios by retransmitting received radio signals

PROBABLE CAUSE

8. Based on my investigation and the facts below, there is probable cause to believe DESALVO stole government property in violation of 18 U.S.C. § 641. The current confirmed value of property stolen totals to $89,943.00. Government property includes the physical items, as well as any government proprietary software, electronic data, information intended to be used for official use only. Additionally, DESALVO violated COMSEC, Operations Security (OPSEC), and INFOSEC policies as a result of his actions and theft of government property, which caused a critical compromise to communications for 17 DoD installations. The violated policies may coincide with additional Title 18 U.S.C violations, that will be evaluated at a later time. The devices outlined in this affidavit were seized based on probable cause as outlined in Attachment A. There is probable cause to search the information contained on the devices seized under Attachment A for evidence, instrumentalities, contraband, or fruits of the crimes as further explained below.

9. In August 2022, my office received a notification from BENJAMIN ROOP, Contractor, Test Support Division, Arnold Air Force Base (AAFB), TN, that he suspected DESALVO possessed government equipment without authorization, and used government equipment for other than official business.

10. On 15 Aug 22, I interviewed DESALVO's co-worker, JOEL THATCHER, Contractor, Land Mobile Radio (LMR) Technician, LMR Shop, AAFB, TN, who stated he was responsible for equipment inventory and noted multiple items were missing and unaccounted for. He witnessed DESALVO conduct unauthorized communications using AAFB LMR equipment. He identified AAFB LMR equipment was in DESALVO's personal vehicle, and DESALVO maintained possession of other LMR equipment items, including controlled COMSEC devices. THATCHER stated other co-workers suspected DESALVO had an LMR workstation at his home, which included equipment from AAFB. THATCHER reported DESALVO twice for insider threat indicators and unauthorized possession of AAFB LMR equipment.

11. On 18 Aug 22, I interviewed DESALVO's co-worker BRIAN HOWELL, Contractor, LMR Technician, LMR Shop, AAFB, TN who stated he knew DESALVO for over 20 years. HOWELL allowed DESALVO to rent one of his properties at 513 McKellar Drive, Manchester, TN, via a gentleman's agreement at $800.00 per month including utilities. DESALVO made approximately $40 per hour and frequently did not pay rent or utilities. HOWELL was angered by DESALVO's missed payments and told him to move out. HOWELL confirmed DESALVO had AAFB LMR equipment in his possession both on and off the installation.

12. In August 2022, I briefed Investigator (Inv) JASON LAYNE, Department of the Air Force Security Forces (DAF/SF), AAFB, TN, on the facts and circumstances of the investigation.

13. In October 2022, the LMR shop conducted a self-audit inventory and identified three missing radios. The radios were suspected to be in DESALVO's possession. HOWELL contacted DESALVO and asked about the missing radios, to which DESALVO confirmed they were in his possession at his residence.

14. In November 2022, DESALVO's upper management, JONATHAN GUERTIN, Program Manager, Abacus Technology Corporation, AAFB, TN, issued an official directive via email that Abacus LMR employees were not authorized to take any AAFB equipment off the installation.

15. In November 2022, OSI Det 106 and DAF/SF briefed AAFB leadership on the facts and circumstances of the investigation. OSI Det 106 recommended DoD oversight initiate a 100% physical inventory of LMR equipment. The inventory revealed over 100 items missing, lost, or stolen. The missing equipment was valued at approximately $150,000.

16. From November 2022 to December 2022, Inv LAYNE briefed the Coffee County Sheriff's Department (CCSD), Manchester, TN, on the facts and circumstances of the investigation.

17. On 27 Jan 23, Inv CODY KOON, CCSD, Manchester, TN, secured search warrants for DESALVO's known residences at 349 Clyde Vickers Rd, Estill Springs, TN, and 513 McKellar Dr, Manchester, TN, based on probable cause that DESALVO and HONEY DESALVO (DESALVO's wife), 349 Clyde Vickers Rd, Estill Springs, TN, were in possession and control of certain evidence of crime to wit: violations of states laws as set forth in Section TCA 39-14-103

Theft of Property over $1,000.00 and that evidence of said crimes would be found at the residences. The evidence items to be searched for were as follows:

a. All Land Mobile Radio (LMR) equipment to include, all mobile radios, portable radios, radio repeaters, telecommunication devices, network devices.

b. Equipment used to program radios to include, programs, CPS (Customer Programming Software), dongles, emulators, other programs used to program LMR, storage devices to include hard drives, flash drives, USB devices, or any other device capable of storing data, and code plugs (programming of LMR).

c. Motorola APX 8000 radios (serial numbers 579CXV0094, 579CXV0097 and 579CXV0098).

d. HP-Gen 7 Serial Number 2TK2140383, HP Elite X2 Serial Number 2TK82901SB.

The search included all persons, outbuildings, locked and unlocked containers, outhouses, trash receptacles, mailboxes, storage buildings, and other outside structures directly related to the locations and all vehicles found thereon, for the aforesaid evidence; and if found the same or any part thereof, investigators shall seize evidence.

18. On 27 Jan 23, the search warrants were executed with the following parties on scene: CCSD to include: Sheriff CHAD PARTON, Inv KOON, Inv BRANDON GULLET, Capt BILLY BUTLER, Inv KERRY FARRAR, Chief Deputy FRANK WATKINS, and Inv ALEX BELL; DAF/SF to include Inv JASON LAYNE, Chief RAY KELLY, and Operations Officer CHRISTOPHER SZATKOWSK; District Attorney (DA) Inv JASON KENNEDY; and SA

TREVOR OSBORN and SA ZACHARY WESLEY, OSI Det 106, AAFB, TN. 131 items in total were seized during the search. On 28 Jan 23, Inv KOON obtained authorization to arrest DESALVO based on the probable cause outlined in the search warrant affidavits, which subsequently confirmed Theft of Government Property over $10,000 during the search of the premises.

19. During the search, I witnessed an active computer screen, containing Motorola radio programming software, which contained the entire AAFB communications system on DESALVO's home network. In addition to AAFB, multiple other agencies in the State of Tennessee were identified on the home network to include FBI, Tennessee Valley Authority (TVA), Tennessee Emergency Management Agency (TEMA), Vanderbilt Hospital, Tennessee Highway Patrol (THP) as well as a plethora of other trunk systems.

20. The evidence items seized were initially sorted by known/confirmed government property, unknown and suspected government property and DESALVO's personal property. Subject matter experts (SME) from AAFB were asked to participate in the identification of AAFB property. OSI Det 106, DAF/SF and AAFB SMEs identified DESALVO had unauthorized administrator access to the Air Education and Training Command (AETC) enterprise LMR (eLMR) system affecting 17 DoD installations. A major command (MAJCOM) represents an Air Force subdivision having a specific portion of the Air Force mission. Each MAJCOM is directly subordinate to Headquarters Air Force. MAJCOMs are interrelated and complementary, providing offensive, defensive, and support elements. The AETC is one of the nine MAJCOMs of the United States Air Force (USAF) reporting to Headquarters Air Force. The AETC eLMR network system managed under the Land Mobile Radio Product Management Office, Air Force Installation and Mission Support Center's Installation Support Directorate (AFIMSC/IZCS), Joint Base San

Antonio (JBSA)-Lackland, TX, possessed administrative control over AETC eLMR communications, which encompassed 17 DoD installations.

21. Interviews of witnesses and co-workers revealed DESALVO sold radios and radio equipment, worked odd hours, was arrogant, frequently lied, displayed inappropriate workplace behavior and sexual harassment, had financial problems, and possessed AAFB LMR equipment.

22. On 7 Feb 23, I briefed the Federal Bureau of Investigations (FBI) on the facts and circumstances of the investigation. The FBI agreed to work jointly with OSI and assist in whatever capacities necessary.

23. On 15 Feb 23, all evidence items seized by CCSD were transferred to OSI Det 106, as the lead investigative agency.

24. On 16 Feb 23, I briefed the United States Attorney's Office (USAO) of the Eastern District of Tennessee on the facts and circumstances of the investigation. The USAO agreed to open a case based on the facts provided.

25. The Devices recovered from DESALVO's residence pursuant to the state search warrant and listed in Attachment A are currently in the lawful possession of OSI. They came into the OSI's possession in the following way: Seized during CCSD search warrants and subsequently transferred to OSI upon case initiation. Based on my training, experience, and research, I know that the Devices listed in Attachment A have capabilities that allow them to serve as means for programming radio systems and associated radio equipment and storing electronic data. In addition to the capabilities mentioned, devices such as the cell phones and laptops can have wide-ranging capabilities to include cameras that can capture photographs and videos, wide-ranging unique electronic applications that can be individually installed on the devices, such as for radio programming, media storage, buying and selling goods, etc., used as a means for communications

between individuals, sending and receiving electronic data. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device, as reflected in Attachment B.

26. The Devices are currently in storage at the OSI Det 106 Evidence Locker at 100 Kindel Drive, Ste. C305, AAFB, TN. In my training and experience, I know that the Devices have been stored in a way its contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of OSI.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

1. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

2. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

3. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted

portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored

on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device to obtain unauthorized access to another electronic device over the Internet, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

4. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

5. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

BIOMETRIC ACCESS TO DEVICES

1. This warrant permits law enforcement to compel BRENT DESALVO to unlock any devices requiring biometric access subject to search pursuant to this warrant. The grounds for this request are as follows:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices

produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes, and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more

convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this Affidavit, your Affiant has confirmation that digital devices were found during the search. The passcode or password that would unlock the Devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the Devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours have elapsed since the device was last unlocked; or (2) when the device has not been unlocked using a fingerprint for 8 hours *and* the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the

opportunity to unlock the device through a biometric feature may exist for only a short time.

h. Due to the foregoing, if law enforcement personnel encounter any Devices that are subject to search pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of DESALVO to the fingerprint scanner of the Devices found at the Premises; (2) hold the Devices found at the premises in front of the faces of DESALVO and activate the facial recognition feature; and/or (3) hold the Devices found at the Premises in front of the face of DESALVO and activate the iris recognition feature, for the purpose of attempting to unlock the Devices in order to search the contents as authorized by this warrant.

CONCLUSION

I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

Trevor J. Osborn
OSI Special Agent
Arnold AFB, TN

Sworn and subscribed before me this 29th day of June 2023.

SUSAN K. LEE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

1. The property to be searched is a Toshiba Hard Drive, serial number: 95513250P; Toshiba Hard Drive, serial number: 96C34369A-1; Hitachi Hard Drive, serial number: DLH7SJNB-1; Seagate Hard Drive, serial number: 5RE26LL0-2; Maxtor Hard Drive, serial number: R20JVAYE; Maxtor Hard Drive, serial number: F12LJHHE-3; Western Digital Hard Drive, serial number: WMA2F; Western Digital Hard Drive, serial number: WCAATC010464; Western Digital Hard Drive, serial number: WMA6Y1263379-1; Unmarked Hard Drive, serial number: 6EG1EVP6; a Seagate External Hard Drive, serial number: NAOM2FQZ; a Seagate Hard Drive, serial number: 6RX6B5YB; a HP Hard Drive, serial number: B365P6A079T5; One cardboard box containing several hard drives; a Seagate Hard Drive, serial number: NAATPFX2; a Seagate Hard Drive, serial number: WXN1AB85Z9RY; a MyPassport External Hard Drive, serial number: NAA863E0; a ONN Hard Drive, serial number: 100003560; a Maxpro writing pen with attached flash drive; One box of multiple electronic memory storage chips derived from computer towers; a Samsung Galaxy S8 Cell Phone, FCOID: A3LSMG950U; a Samsung Cell Phone, model number unknown, IMEI: 357452522814468; Several Compact Discs, a Dell Laptop Computer, serial number: 221TWZ1; a Dell Inspiron Laptop, serial number: 00043726386389; 14 Thumb Drives collected in a black case; a HP Envy computer tower, serial number: 2MD61302TZ; a HP Laptop Computer, serial number: CND1Q3472L; a HP Laptop Computer, serial number: CND10348BR; a HP ProLiant Computer Tower, serial number: MX244500MX; a HP Pavilion Computer Tower, serial number: CNV6440K5L; a HP Z420 Computer Tower, serial number: 2UA4431ND9; a HP Z440 Computer Tower, serial number: 2UA5251RWR; a KVL-4000, serial number: 201CQH3355; Three SD Memory Cards, SanDisk, Wintec and Mad Catz; a Seagate NAS 4-bay hard drive reader serial number: NA6A50ZJ with three hard drives inside serial number's

W1H4597X, W1H45A85, W1H45A01; a Seagate NAS 4-bay hard drive reader serial number: NA6A50ZC with four hard drives inside, serial numbers: W1H45AWM, W1H45AZY, W1H4590M, W1H45AY5; a Motorola XTS5000 Portable Radio, serial number removed from device; a Windows 2012 R2 Thumb Drive; an unmarked Thumb Drive, silver and black in color; Five Thumb Drives identified as programming software for AAFB LMR communications systems and Tennessee Advanced Communications Network (TACN) communications systems; hereinafter the "Devices." The Devices are currently located at the OSI Det 106 Evidence Locker at 100 Kindel Drive, Ste. C305, AAFB, TN.

2. Items were seized based on the documentation included with this attachment.

3. This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of Title 18 U.S.C. § 641, and involve DESALVO since his employment at AAFB, including:

a. Computers or storage media used or able to be used as a means to commit the violations described above.

b. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which are stored records or information that is otherwise called for by this warrant;

c. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

d. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

e. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

f. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;

g. evidence of the attachment to the Devices of other storage devices or similar containers for electronic evidence;

h. evidence of the use of cloud storage, including Apple iCloud;

i. evidence of programs (and associated data) that are designed to eliminate data from the Devices;

j. evidence of the times the Devices were used;

k. passwords, encryption keys, and other access devices that may be necessary to access the Devices;

l. documentation and manuals that may be necessary to access the Devices or to conduct a forensic examination of the Devices or that show the operation of AAFB and other government communications systems;

m. records of or information about Internet Protocol addresses used by the Devices;

n. records of or information about the Devices' Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

o. contextual information necessary to understand the evidence described in this attachment;

p. Routers, modems, and network equipment used to connect computers to the Internet.

q. Records, information, and items relating to the ownership or use of the Devices and equipment, including sales receipts, bills for Internet access, and handwritten notes;

r. Radio programming software and related identifying information pertaining to LMR communications systems;

s. types, amounts, and prices of any sold radio equipment as well as dates, places, and amounts of specific transactions;

t. any information related to the storage of electronic data belonging to AAFB;

u. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;

v. all bank records, checks, credit card bills, account information, and other financial records associated to the sale of radio equipment.

2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

a. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

3. During the execution of the search, law enforcement personnel are also specifically authorized to compel BRENT DESALVO, date of birth 20 Dec 74, to provide biometric features, including pressing his fingers (including thumbs) against and/or putting his face before the sensor, or any other security feature requiring biometric recognition, of any of the Devices found at the PREMISES which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments, for the purpose of attempting to unlock the Devices' security features in order to search the contents as authorized by this warrant.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, OSI may deliver a complete copy of the seized or copied

electronic data to the custody and control of attorneys for the government and their support staff for their independent review.